

IMMUNE SYSTEM BASED INTRUSION DETECTION SYSTEM

Christoph Ehret, Ulrich Ultes-Nitsche

University of Fribourg
Department of Computer Science, University of Fribourg,
Boulevard de Pérolles 90,
CH-1700 Fribourg, Switzerland
{christoph.ehret,uun}@unifr.ch

ABSTRACT

The threats and intrusions in IT systems can basically be compared to human diseases with the difference that the human body has an effective way to deal with them, what still need to be designed for IT systems. The human immune system (HIS) can detect and defend against yet unseen intruders, is distributed, adaptive and multilayered to name only a few of its features. Our immune system incorporates a powerful and diverse set of characteristics which are very interesting to use in the design of Intrusion Detection Systems (IDS). The authors propose therefore a hybrid intrusion detection system which combines host based and network based components but giving the focus to the host based intrusion detection as it is similar to the HIS. The proposed intrusion detection system will use the concepts of the artificial immune systems (AIS) which is a promising biologically inspired computing model based on the HIS. This paper presents an intrusion detection system based on the model of the human immune system and which will use the artificial immune systems paradigm. Furthermore the paper will also introduce some yet unused AIS concepts that can be applied to improve the effectiveness of IDS.

KEY WORDS

Intrusion detection systems, immune system, artificial immune system.

IMMUNE SYSTEM BASED INTRUSION DETECTION SYSTEM

1 INTRODUCTION

Intrusion detection systems (IDS) are nowadays very important for every IT company which is concerned with security and sensitive systems. Even if a lot of research was already done on this topic, the perfect IDS has still not been found and it stays a hot and challenging area in computer security research. Recently a new approach started to make its way to intrusion detection, namely the immune system. It has a lot of interesting features we would like to find in IDS. A new artificial intelligence paradigm was created from the immune system, namely the artificial immune system; this paradigm is rather new compared to neural networks or fuzzy logic, but it is very promising for different areas in computer science. If we abstractly compare the way an intrusion detection system and the human immune system work, we can actually find quite some similarities. Within this context it is normal to use as much similarities as possible to improve IDS and to see how we can implement the different features; this is where the artificial immune systems paradigm will help.

In this paper, we describe work in progress on artificial-immune-system inspired IDS. Its main purpose is to motivate the new paradigm and highlight the benefit one expects from that paradigm. The paper is structured as follows. First, we present the common design of the intrusion detection systems. Next, we give a brief overview of the immune system followed by a brief introduction to artificial immune systems. Then we discuss similarities between IDS and the immune system and their impact on advanced IDS. Finally, we conclude with presenting future work.

2 INTRUSION DETECTION SYSTEMS

An intrusion detection system can be compared with a house burglar alarm: if somebody tries to enter illegally in the house, one of the sensors will detect it what will trigger the alarm bell and alert the house owner and the

police. Similarly, if somebody tries to compromise the confidentiality, the integrity or the availability of a computer system or network, or tries to break the security protections, an intrusion detection system will alert the system owner and the security team [1].

Intrusion detection is the process of monitoring and analysing events of a computer system or network and tries to find intrusions. Events like trying to break into a system from the Internet using software exploits or trying to gain higher privileges on a system are representative events that will be recognized as an intrusion. Highly sensitive systems that have to be protected against 0-days attacks or critical systems with high availability needs, which cannot be patched very often, are typical systems that need an IDS. It is important to understand that the goal of an IDS is not to prevent an attack, but to detect it as quickly as possible and alert the right people who can then take the appropriate measures if a system was compromised; automatic measures can sometimes also be used by the IDS.

2.1 Placement

The placement or audit source location is one of the IDS taxonomies [2] the authors will focus on. There are two different strategies where to place intrusion detection systems: on a host or on a network node. Both placement strategies have their advantages and disadvantages.

A host-based IDS (HIDS) is often an application installed on the host for monitoring purposes, like Snort [3], Samhain [4] or Prelude [5]. It analyses events from running applications, the operating system, network packets or logs and if an intrusion is detected, an alarm event is sent to a central monitoring instance.

A network-based IDS (NIDS), often a commercial product installed on some special hardware, is positioned on a network node. It captures and analyses network packets that go through the node it monitors. One single NIDS or sensor, intelligently placed, can monitor several hosts independently of their operating system [7]. The captured network packets are analysed locally and if an attack is detected, an alarm event is sent to a central monitoring instance.

Table 1 lists in parallel the advantages and disadvantages of both host based and network based IDS, regarding several typical features.

Table 1. Advantages and disadvantages of HIDS and NIDS

Features	HIDS	NIDS
Management	Harder to manage due to the heterogeneity of the environment and its high number in large networks with many hosts	Simple to manage due to its homogeneity and a few NIDS are sufficient to monitor a large network with many hosts
Analyse encrypted network traffic	YES	NO
IDS evasion techniques	Harder to perform than on NIDS[6]	Evasion techniques like fragmentation will easily work with NIDS when they have no possibility to reconstruct locally the fragmented network packets
Knows if an attack was successful or not on a host	YES	NO
Protection against targeted attacks	Can be disabled during the attack of a host or by specific denial-of-service attacks	Easier than HIDS to protect against targeted attacks and can run in stealth mode
Detects large network attacks	NO	YES
Uses computing resources of the monitored host	YES	NO

It is not easy to decide between HIDS and NIDS which one is better or suites best our needs, but the trend is to integrate both or to design hybrid IDS that have both components [5][8]. Table 1 will help us to understand the proposed IDS design presented later.

2.2 Detection mechanisms

The detection mechanisms or algorithms represent another IDS taxonomy the authors will focus on. There are two different detection mechanisms IDS can use to find intrusions or attack attempts: the misuse detection and the anomaly detection.

The misuse detection approach, the most used in commercial products, monitors and analyses system events looking for a known event or sequence of events that represents an attack; this event or sequence of events is stored in the form of a signature. One disadvantage of the misuse detection is that if the signatures database is not up to date or if a new attack is used for which there exists no signature yet, the IDS will find nothing suspicious. On the other hand theses signatures permit to define an attack precisely and to give it a name, what really helps system administrators without great security background to understand what happened and if needed inform the security team. Another problem that can exist is if the signatures are too specifically bound to a given attack, the IDS will not be able to detect variants of the attack. It is nevertheless due to this specificity that the false positive or false alarms rate is very low.

The anomaly detection approach detects unusual behaviours, i.e. anomalies, like a great CPU consumption that lasts longer than usual, a high network traffic from the secretary's computer at 4am or the number of files accessed by a user in a given period of time. In order to detect anomalies, the detection system needs to create a normal behaviour profile and train the system on it. The anomaly detection can then use statistical measures or rules and compare the results with the profile; if there are differences, an anomaly was detected. This detection approach is rarely used in commercial products but is of great interest in the research area of intrusion detection. One advantage of this detection mechanism is that it is possible to detect yet unknown attacks and generate immediately a signature from it for the

misuse detection. The false positive and false negative rate of the anomaly detection is unfortunately much higher than with the misuse detection.

3 IMMUNE SYSTEM

3.1 Overview

The human immune system (HIS) is quite complex and elaborate. The defence of the HIS is organised in different layers, mainly the exterior defences, which are biochemical and physical barriers like for example skin or bronchi, the physiological barrier, where pH and temperature provide inappropriate living conditions for pathogens, the innate system and finally the adaptive system. Every layer has different defence mechanisms and stops different types of pathogens. The innate and adaptive systems are again divided into several different cells, as we can see it on Figure 1.

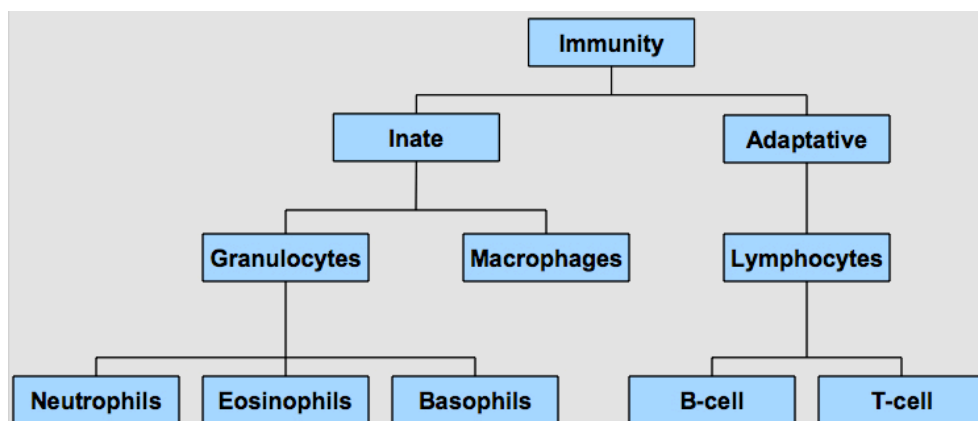


Figure 1. Major immune cells and their classification

Every leukocyte has very specific functions, like for example the Neutrophil¹ which migrates to sites of inflammation or infection and ingests micro organisms or particles, destroys them and dies, or the Eosinophil² which is responsible to combat parasites and is the main effector in allergic responses and in asthma. The B- and T-cells are the actors of the adaptive

¹ The Neutrophils constitute the majority of blood leukocytes and are part of the phagocyte cells

² The Eosinophil constitutes 1-5% of blood leukocytes

system; they are responsible to detect yet unknown pathogens, produce the specific antibodies and destroy them. Every B- and T-cells have different detectors, called epitopes, which interact with different kind of pathogens.

In order to improve the diversification, new B- and T-cells die and are created with randomly generated receptors every day, what modifies continuously the set of possible detected pathogens. There is a great interaction between all the different cells of the HIS; some immune cells secrete special substances that will attract some other type of immune cells, or some are responsible to produce an inflammation what will allow more immune cells to reach this particular region.

For more information on the different leukocytes and their role within the HIS consult [9].

3.2 Artificial Immune Systems

We can find quite different definitions of an artificial immune system (AIS) in the literature; one possible definition could be "*Artificial immune systems (AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving*" [10]. The artificial immune system paradigm is rather recent comparing to other artificial intelligence paradigms like Neural Networks, Fuzzy Logic or the genetic algorithms. AIS began in 1986 with Farmer, Packard and Perelson's paper on immune networks [11], but there was only in the mid-90's that it kept the attention of scientists.

What do we need if we want to implement an AIS framework? If we abstract the immune system in a simplistic way we have a population of different types of immune cells and interactions between them through receptors. For our AIS we therefore need to have a population, defined as a set, a way to describe each element of the set, its length, and a way to measure an interaction. To describe the population we will use the concept of *shape space* (S); it is used in immunology to quantitatively describe the interactions between immune cells and antigens. An element of S is described by a set of N_p parameters (length, width, charge, ...). To cover the whole shape-space, we actually need to generate $N = k^L$ different elements, where k is the size of the alphabet, L the length of one element of the set, and N is called the *potential repertoire*. As we have seen, one antibody can detect pathogens with similar structure, i.e. it is not bound to only one

specific pathogen (imagine the number of antibodies we would need if each could detect only one given pathogen). For that we will introduce the notion of *coverage*; $C = \sum_{i=0}^{L-\varepsilon} \frac{L!}{i!(L-i)!}$ gives us the number of antigens covered by one antibody, where L is the string length of the antibody and ε the *cross-reactivity threshold*. The cross-reactivity threshold characterizes the fact that each antibody interacts with all antigens whose complement lies within a small surrounding region. The minimum elements necessary to cover the shape-space S is therefore given by $N_m = \text{ceil}(\frac{N}{C})$, where N is the potential repertoire and C the coverage. The interaction, i.e. the affinity between an antibody and an antigen, both of length L , is evaluated with a distance measure between their attribute strings $S^L \times S^L \rightarrow \mathbb{R}^+$. To measure the distance, the Euclidean, Manhattan or Hamming distance functions are often used. Finally, the training phase is often done like in the immune system using the negative selection [12] improved sometimes with some genetic algorithms. In the immune system, T-cells are trained in the thymus and selected or matured using the negative selection process depending if they reacted or not to *self* cells; if T-cells recognized the own cells (self-cells) as intruders they will not be selected and will not survive the training phase.

The application domain of AIS is becoming quite large. It is used for example in computer security, data analysis, search and optimization methods, agent-based systems, or autonomous navigation and control systems.

4 IMMUNE SYSTEM ANALOGY TO IDS

The human immune system has abstractly quite some similarities with intrusion detection systems, what the authors think make it naturally a good candidate as model for IDS design. The innate system of the human immune system can be compared with the misuse detection of the IDS; both uses pattern recognition based respectively on memory cells or signatures database to detect intrusions. The adaptive system can be compared with the anomaly detection where both can detect yet unseen attacks and where their sensors have to go through a training phase. Following the immune system model, the authors propose an IDS that uses both misuse and anomaly detection, quite the contrary of traditional IDS design that uses either misuse or anomaly detection. The misuse detection part will contain only the signatures for the running services and the anomaly detection sensors will

be able to generate automatically new signatures of detected and yet unknown attacks.

Each immune system protects a particular body and is also located in that same body. If we compare this to IDS placement strategy we clearly have a host-based IDS. Therefore the authors propose a HIDS with the possibility to send newly generated signatures to other hosts on a same LAN. Thanks to this feature, we include two important characteristics of the immune system that are distributivity and diversity. Moreover this permits us to abstract a LAN as a body and each host of this LAN becomes an immune cell.

One of the seven IDS requirements reported in Kim [13] is *efficiency*. An IDS has of course to be simple and not use too many resources on the monitored system; to this statement we would append “when nothing anomalous happens on this system”. What happens to a human being when he has a cold with fever and a nasty headache? He stays in bed and tries to recover as quick and good as possible; he perhaps boils some water for his tea or eats a little bit but that is all he will do until he has recover strength. The authors propose to build an IDS that follows this principle: when something anomalous happens on a system it will slow down its normal functioning and give more resources to the IDS in order to find the problem, possibly fix it and avoid on the same way that the hypothetical attack can spread too quickly. This will also help the response team to take appropriate measures.

5 CONSEQUENCES FOR ADVANCED IDS

Lundin and Jonsson identified nine research issues in the intrusion detection area [14]: foundations, data collection, detection methods, reporting and response, IDS environment and architecture, IDS security, testing and evaluation, operational aspects and social aspects. The authors of the paper focus their research using the AIS paradigm on the issues *detection methods* and *IDS security*. The detection method issue is simple to implement with AIS using the negative selection we have seen previously or using ideas from the danger model, another model in immunology we have not described here and that is out of scope of this paper. This other model is quite promising and has yet not been used often in AIS [15]. As we have seen in the previous section, we will introduce a new intrusion detection

approach using both misuse and anomaly detection with automatic signature generation. This approach was partially implemented in ADENIDS [16], but it was limited to generate signatures for buffer overflows and was done at a high level of abstraction. Furthermore using both detection approaches together with the co-stimulation mechanism of the immune system will help to reduce the false positives. We will have to go much deeper at a level quite similar to the way the immune system works and auto-generation of signature files for SNORT is foreseen.

The *IDS security* issue can be implemented in artificial immune systems using multiple independent sensors in different places of the system like for example with agents or the co-stimulation mechanisms we have seen in section 3. With this issue we have the multilayered or defence in depth feature of the immune system, the diversity of different kinds of detectors and we can minimize or avoid single points of failure.

6 CONCLUSION

The immune system is complex but very powerful; it can detect a lot of different types of pathogens, even unknown one, and thanks to a strong interaction between all the different actors of the immune system the pathogens can be destroyed. As the immune system has some very interesting features, a new artificial intelligence paradigm called the artificial immune system was created from it. Computer security, especially the antivirus and IDS fields, is of course an interesting candidate to apply AIS. The immune system itself is actually a very interesting approach to intrusion detection.

We discussed in this paper an immune-system-inspired approach to intrusion detection. The similarities between the tasks of the human immune system and intrusion detection systems suggest that IDS can be improved by converting concepts from the biological to the digital world. Clearly, we must abstract from the concrete biological principals to benefit from them in intrusion detection. It was the purpose of this paper to discuss these necessary abstractions. Interaction between misuse and anomaly detection, distributivity, avoiding single points of failure, and locality, possibly affecting only single processes, are what we have extracted as main features of immune-system-inspired IDS.

Our current research in direction focuses on identifying good anomaly detection methods for IDS. This includes particularly reducing the number of false positives in the potentially applicable methods, as they are usually the limiting factor in misuse detection, and not the false negatives that are much easier to control.

7 REFERENCES

- [1] R. Bace and P. Mell. "Intrusion Detection Systems", NIST Special Publication 800-31. 2001.
- [2] H. Debar, M. Dacier and A. Wespi. "Towards a taxonomy of intrusion-detection systems". *Computer Networks*, April 1999.
- [3] Snort
URL: <http://www.snort.org>
- [4] Samhain
URL: <http://www.la-samhna.de/samhain>
- [5] Prelude
URL: <http://prelude-ids.org>
- [6] T. H. Ptacek and T. N. Newsham. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", Report from Secure Networks Inc., 1998.
- [7] J. McHugh. "Intrusion and intrusion detection", *International Journal of Information Security*, vol. 1, pp. 14-35, 2001.
- [8] S. Northcutt and J. Novak. "Network Intrusion Detection", Sams, Third Edition, 2002.
- [9] I. Roitt, J. Brostoff and D. Male. "Immunology", Mosby, Sixth Edition, 2001.
- [10] L. N. de Castro and J. Timmis. "Artificial Immune Systems: A New Computational Intelligence Approach", Springer, 2002.
- [11] J.D. Farmer, N. Packard and A. Perelson. "The immune system, adaptation and machine learning", in *Physica D*, vol. 2, pp. 187-204, 1986.

- [12] S. Forrest, A. Perelson, L. Allen and R. Cherukuri. "Self-Nonself Discrimination in a Computer", in *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, 1994.
- [13] J.W. Kim. "Integrating Artificial Immune Algorithms for Intrusion Detection", PhD thesis, University College London, 2002.
- [14] E. Lundin and E. Jonsson. "Survey of Intrusion Detection Systems", Technical Report 02-04, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 2002.
- [15] U. Aickelin, P. Bentley, S. Cayzer, J. Kim and J. McLeod. "Danger Theory: The Link between AIS and IDS?", in *Proceedings of the Second International Conference, ICARIS 2003* (LNCS 2787), pp. 147-155, Springer, 2003.
- [16] F. S. de Paula, L. N. de Castro and P. L. de Geus. "An Intrusion Detection System Using Ideas from the Immune System", in *Evolutionary Computation*, vol. 1, pp. 1059-1066, 2004.